

IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): An information providing device comprising:
a provider association unit configured to associate making a plurality of information providers, including first and second information providers, ~~be associated with each other~~, the plurality of information providers providing respective user information items, the provider association unit comprising:

a first unit causing the first information provider to receive a first user information item, stored in a first information management unit, in response to a user information receiving request;

a second unit causing the second information provider to receive a second user information item, correlated with the first user information item and stored in a second information management unit, in response to a predetermined identification data; and

a third unit configured to generate an authentication ticket including data indicating at least one of an authentication provider name, a term of validity of the ticket, an authentication domain name, and user attributes outputting a unified information item which is created by combining the first user information item and the second user information item based on the predetermined identification data; and an interface configured to transmit the authentication ticket to a computer remote from the information providing device via a network,

~~werein the second information provider receives the second user information item only when the user information receiving request exceeds a range of validity associated with the first information provider.~~

Claim 2 (Original): The information providing device according to claim 1 wherein the user information receiving request contains retrieval conditions specified therein, and the provider association unit causes the first and second information providers to respectively receive the first and second user information items that satisfy the retrieval conditions.

Claim 3 (Original): The information providing device according to claim 1 wherein the provider association unit is provided to unify the information items received by the first and second information providers for every user.

Claim 4 (Previously Presented): The information providing device according to claim 1 wherein the information providing device further comprises:

the first information provider and
the second information provider.

Claim 5 (Previously Presented): The information providing device according to claim 1 wherein the information providing device further comprises:

a first-information-provider information management unit managing a first-information-provider identification data which identifies the first information provider from among the plurality of information providers; and
a second-information-provider information management unit managing a second-information-provider identification data which identifies the second information provider from among the plurality of information providers.

Claim 6 (Previously Presented): The information providing device according to claim 1 wherein the information providing device further comprises:

a call information management unit in which a plurality of call information items used to call the plurality of information providers respectively are recorded, and

the provider association unit causes the first and second information providers to respectively receive the first and second information items by calling the first and second information providers based on the call information management unit.

Claim 7 (Currently Amended): An information providing method for use in an information providing device which makes a plurality of information providers, including first and second information providers, be associated with each other, the information providing method comprising:

causing the first information provider to receive a first user information item, stored in a first information management unit, in response to a user information receiving request;

causing the second information provider to receive a second user information item when the user information receiving request exceeds a range of validity associated with the first information provider, the second user information item is correlated with the first user information item and stored in a second information management unit, in response to a predetermined identification data; and

outputting generating an authentication ticket including data indicating at least one of an authentication provider name, a term of validity of the ticket, an authentication domain name, and user attributes a unified information item which is created by combining the first user information item and the second user information item based on the predetermined identification data; and

transmitting the authentication ticket to a computer remote from the information providing device via a network.

Claim 8 (Original): The information providing method according to claim 7 wherein the user information receiving request contains retrieval conditions specified therein, and the first and second information providers are caused to respectively receive the first and second user information items that satisfy the retrieval conditions.

Claim 9 (Original): The information providing method according to claim 7 wherein the information items received by the first and second information providers are unified for every user.

Claim 10 (Currently Amended): A tangible storage recording medium including computer program instructions for causing an information providing device which makes a plurality of information providers, including first and second information providers, be associated with each other, to perform:

causing the first information provider to receive a first user information item, stored in a first information management unit, in response to a user information receiving request;

causing the second information provider to receive a second user information item when the user information receiving request exceeds a range of validity associated with the first information provider, the second user information item is correlated with the first user information item and stored in a second information management unit, in response to a predetermined identification data; and

outputting generating an authentication ticket including data indicating at least one of an authentication provider name, a term of validity of the ticket, an authentication domain name, and user attributes a unified information item which is created by combining the first user information item and the second user information item based on the predetermined identification data; and

transmitting the authentication ticket to a computer remote from the information providing device via a network.

Claim 11 (Currently Amended): The tangible storage recording medium including computer program instructions according to claim 10 wherein the user information receiving request contains retrieval conditions specified therein, and the first and second information providers are caused to respectively receive the first and second user information items that satisfy the retrieval conditions.

Claim 12 (Currently Amended): A user authentication device comprising:
a provider association unit which makes a plurality of authentication providers, including first and second authentication providers, be associated with each other, the provider association unit comprising:
a first unit causing the first authentication provider to perform, in response to a first authentication request, a first user authentication based on a first user identification data that is specified in the first authentication request; and
a second unit causing the second authentication provider to perform, in response to a second authentication request related to a user approved by the first user authentication, a second user authentication based on a second user identification data that is correlated with the first user identification data[,]; and

a third unit configured to generate an authentication ticket including data indicating at least one of a ticket type, an authentication provider name, a term of validity of the ticket, and an authentication domain name based on a result of the first and second user authentication; and

an interface configured to transmit the authentication ticket to a computer remote from the information providing device via a network

~~wherein the second authentication provider performs the second user authentication only when a user information receiving request exceeds a range of validity associated with the first authentication provider.~~

Claim 13 (Previously Presented): The user authentication device according to claim 12 wherein the user authentication device further comprises:

the first authentication provider and
the second authentication provider.

Claim 14 (Previously Presented): The user authentication device according to claim 12 wherein the user authentication device further comprises:

a user-identification management unit in which the first user identification data and the second user identification data are correlated to each other and recorded, and
the provider association unit is provided to search for the second user identification data in the user-identification management unit based on the first user identification data.

Claim 15 (Previously Presented): The user authentication device according to claim 12 wherein the provider association unit further comprises:

a user-identification management unit in which the first user identification data and the second user identification data are correlated to each other and recorded, and
the provider association unit is provided to search for the second user identification data in the user-identification management unit based on the first user identification data.

Claim 16 (Original): The user authentication device according to claim 12 wherein the user authentication device further comprises:

a first-authentication-provider information management unit managing a first-authentication-provider identification data which identifies the first authentication provider from among the plurality of authentication providers; and

a second-authentication-provider information management unit managing a second-authentication-provider identification data which identifies the second authentication provider from among the plurality of authentication providers.

Claim 17 (Previously Presented): The user authentication device according to claim 12 wherein the user authentication device further comprises:

a call information management unit in which a plurality of call information items used to call the plurality of authentication providers respectively are recorded, and

the provider association unit causes the first and second authentication providers to perform the first and second user authentications respectively by calling the first and second authentication providers based on the call information management unit.

Claim 18 (Original): The user authentication device according to claim 12 wherein the first authentication provider creates a first electronic ticket which certifies approval of the user by the first authentication provider, the second authentication provider creates a second electronic ticket which certifies approval of the user by the second authentication provider, and the user authentication device provides information containing the first electronic ticket, in response to the first authentication request and provides information containing the second electronic ticket, in response to the second authentication request.

Claim 19 (Original): The user authentication device according to claim 18 wherein the provider association unit creates a merge ticket in which the first electronic ticket and the second electronic ticket are unified, and the user authentication device provides a first merge ticket in which the first electronic ticket is unified, in response to the first authentication request, and provides a second merge ticket in which the second electronic ticket is unified further, in response to the second authentication request.

Claim 20 (Original): The user authentication device according to claim 19 wherein the user authentication device provides the merge ticket which is encoded.

Claim 21 (Original): The user authentication device according to claim 19 wherein at least one of the merge ticket, the first electronic ticket, and the second electronic ticket contains a term of validity.

Claim 22 (Original): The user authentication device according to claim 19 wherein at least one of the merge ticket, the first electronic ticket, and the second electronic ticket contains a code for ticket falsification check.

Claim 23 (Cancelled).

Claim 24 (Original): The user authentication device according to claim 12 wherein the first authentication provider is a password authentication provider which performs a password authentication based on a password of the user, and the second authentication provider is a fingerprint authentication provider which performs a fingerprint authentication based on a fingerprint of the user.

Claim 25 (Original): The user authentication device according to claim 19 wherein the provider association unit causes the first authentication provider to decode the first electronic ticket of the first merge ticket in response to a decode request of the first merge ticket, and causes the second authentication provider to decode the second electronic ticket of the second merge ticket in response to a decode request of the second merge ticket.

Claim 26 (Original): The user authentication device according to claim 12 wherein the provider association unit is provided with a call function using a remote procedure call of SOAP.

Claim 27 (Currently Amended): A user authentication method for use in a user authentication device which makes a plurality of authentication providers, including first and second authentication providers, be associated with each other, the user authentication method comprising:

causing the first authentication provider to perform, in response to a first authentication request, a first user authentication based on a first user identification data that is specified in the first authentication request; and

causing the second authentication provider to perform, in response to a second authentication request related to a user approved by the first user authentication, a second user authentication based on a second user identification data that is correlated with the first user identification data;

generating an authentication ticket including data indicating at least one of a ticket type, an authentication provider name, a term of validity of the ticket, and an authentication domain name based on a result of the first and second user authentication; and

transmitting the authentication ticket to a computer remote from the information providing device via a network
~~, wherein the second authentication provider performs the second user authentication only when a user information receiving request exceeds a range of validity associated with the first authentication provider.~~

Claim 28 (Previously Presented): The user authentication method according to claim 27 wherein the second user identification data is searched for in a user-identification management unit, based on the first user identification data, and, in the user-identification management unit, the first user identification data and the second user identification data are correlated to each other and recorded.

Claim 29 (Original): The user authentication method according to claim 27 wherein the first authentication provider is identified from among the plurality of authentication providers based on a first-authentication-provider identification data managed by a first-authentication-provider information management unit, and the second authentication provider is identified from among the plurality of authentication providers based on a second-authentication-provider identification data managed by a second-authentication-provider information management unit.

Claim 30 (Original): The user authentication method according to claim 27 wherein the first and second authentication providers are caused to perform the first and second user authentications respectively by calling the first and second authentication providers based on a call information management unit in which a plurality of call information items used to call the plurality of authentication providers respectively are recorded.

Claim 31 (Currently Amended): A tangible storage recording medium including computer program instructions for causing a user authentication device which makes a plurality of authentication providers, including first and second authentication providers, be associated with each other, to perform:

causing the first authentication provider to perform, in response to a first authentication request, a first user authentication based on a first user identification data that is specified in the first authentication request; and

causing the second authentication provider to perform, in response to a second authentication request related to a user approved by the first user authentication, a second user authentication based on a second user identification data that is correlated with the first user identification data;

generating an authentication ticket including data indicating at least one of a ticket type, an authentication provider name, a term of validity of the ticket, and an authentication domain name based on a result of the first and second user authentication; and

transmitting the authentication ticket to a computer remote from the information providing device via a network

~~, wherein the second authentication provider performs the second user authentication only when a user information receiving request exceeds a range of validity associated with the first authentication provider.~~

Claim 32 (Currently Amended): The tangible storage recording medium including computer program instructions according to claim 31 wherein the second user identification data is searched for in a user-identification management unit, based on the first user identification data, and, in the user-identification management unit, the first user

Application No. 10/803,896

Reply to Office Action of December 14, 2007

identification data and the second user identification data are correlated to each other and

recorded.